REMARKS

This amendment is responsive to the Office Action[1] having a mailing date of December 1, 2005. Claims 1-6 and 8-22 were presented for examination and were rejected. All independent claims, namely claims 1, 5, 9, 13, 14 and 22, are currently amended. Support for these amendments can be found in the application as originally filed; no new matter is added. No claims are canceled. No claims are added. Thus, claims 1-6 and 8-22 are pending.

Claims 1-6 and 8-22 are rejected under 35 U.S.C. § 102(b) as being anticipated by Sudia et al. (U.S. Patent No. 5,825,880; hereinafter Sudia). The rejection is respectfully traversed because all claim elements of the independent claims are not disclosed or suggested by Sudia, for the following reasons.

Consider currently amended claim 1:

> In a node operative within a network of a plurality of nodes, a method for performing cryptographic-related functions, comprising: executing an application program at the *node* which is *not secured*; receiving an input requiring cryptographic-related processing; generating a message via the application program based on the input, the message representing one of a predefined set of messages for *processing by a cryptographic processing component located within the node*; transmitting the message to the cryptographic processing component; and performing the cryptographic-related processing by the cryptographic processing component. (Emphasis added.)

Claim 1 calls for, interalia, (1) executing an application program at a node that *is not secured* and (2) processing a message generated from the application program by a *cryptographic processing component located within the node*. But, Sudia does not

[1] The Office Action may contain a number of statements characterizing the cited references and/or the claims which Applicants may not expressly identify herein. Regardless of whether or not any such statement is identified herein, Applicants do not automatically subscribe to, or acquiesce in, any such statement.

disclose or suggest executing an application program at a node which is not secured while processing a message by a cryptographic processing component located within that node. The Office Action, page 3, refers to a first section of Sudia, col. 9, lines 9-13, to allegedly show processing by Applicants' recited "cryptographic processing component." This first section is contained within a larger section of Sudia col. 8, line 63 - col. 9, line 23, to allegedly show Applicants' recited "within the node" processing.

In Fig. 3 of Sudia, to which these passages relate, there is depicted a single micro-chip which "may also include an optional 'crypto-unit' 46, which is a special purpose arithmetic accelerator unit having hardware for performing accelerated exponentiation and other arithmetic operation of encryption/decryption and signature processes." (Col. 9, lines 9-13). Applicants submit that this brief and vague description of certain cryptographic functionality does not amount to disclosing Applicants' recited "cryptographic processing component."

Moreover, even if this did amount to disclosing a "cryptographic processing component" it still does not disclose such component within a node that is *not secure* as claimed by Applicants. To the contrary, Sudia's smart card is tauted as being secure: "Each such computer or terminal will have a card reader 53, and each operator will have a *secure* 'smart card' 55. Each smart card 55 *securely* contains a private decryption key and a private signature key which are unique to that smart card." (Sudia, Col. 8, lines 23-27, Emphasis added.)

Accordingly, if the Office Action takes the position that this brief and vague description of certain cryptographic functionality necessarily means that the authorizing agent and the signing device are together on the smart card (i.e., allegedly together on the

same node), they would then co-exist in a necessarily *secure* environment on that same node. Furthermore, this position would have to be asserted despite a principal teaching of Sudia that the authorizing agent and the signing device are required to be separated for security purposes, and are separated even to the extent that the signing device of, e.g., Fig. 1, is located in a physically secure location such as a *vault* (Sudia. Col. 7, lines 24-25). Clearly, Sudia does not anticipate Applicants' claim 1 because Sudia requires a secure environment[2] while Applicants' claim 1 is oppositely limited to a non-secure environment.

Applicants' claim amendment language, "...the node is not secured" is supported by the application as originally filed. For example, in Applicants' specification, page 6, lines 1-3, it discusses the nodes 110, 120, and 130 of Fig. 1, such nodes along with server 140 and network 150 comprising Applicants' system. As stated therein, those nodes can be any type of computer device. For example, as disclosed therein, those nodes can be "a personal computer, a laptop, a personal digital assistant (PDA) or a similar device with a connection to network 150." Clearly, these examples of nodes from which Applicants' claimed subject matter can be implemented are not used in a secure environment - e.g., people using a laptop or a PDA do not first find their way to a "vault" and then place themselves with their laptop or PDA inside the vault for security purposes before operating their laptop or PDA. Far to the contrary, laptops and PDA's are used in virtually all public spaces such as, for example, airports, airplanes, trains and train

[2] "Although less preferred, the signing device 39 and message server 47 could be implemented as separate tasks on a single computer *in a highly secure environment*." (Sudia, Col. 7, lines 62-65, Emphasis added.)

stations, buses and bus depots, taxis, hotels lobbies, corporate business environments, etc. Therefore, Applicants' specification as originally filed clearly supports the notion that the "nodes" of its system are used without their being secured, as recited in amended claim 1.

Sudia itself reinforces the fact that personal computers and the like are operated in unsecured areas. "Fig. 3 illustrates a working station for authorizing agents. The human operators who act as authorizing agents may work in relatively *unsecured* areas at desk-top [personal] computers or terminals 51 typically found in a business office." (Sudia, column 8, lines 20-23, Emphasis added.)

In the Office Action, "Response to Arguments" on page 13, the Examiner advises that the limitation "need not be highly secured" is no different from the limitation "not highly secured". Applicants disagree because there is clearly a difference between these two limitations in both the number of words and in the meaning of those words. But, this point is moot in view of the current amendment to claim 1, providing: "not secured." *The Examiner further admits on page 13 of the Office Action that both limitations read on executing the application program at the node which is still secured and "thus does not read on executing the application program on the node that is unsecured."* Based on this admission, with which Applicants agree, Sudia does not read on Applicants' currently amended claim 1.

In the Office Action, "Response to Arguments" on page 14, the Examiner advises that "not highly secure" has not been given patentable weight because the recitation occurs in the preamble. To the contrary, in claim 1, even before the current amendment to claim 1, the "not highly secure" recitation occurred NOT in the preamble, but in the body of the claim. With respect to that claim, the Examiner should have previously given

the limitation patentable weight in the prior office action and should currently give the limitation patentable weight in response to this instant Rule 116 amendment.

It is respectfully submitted that Sudia does not anticipate claim 1 because it does not disclose or suggest at least the claimed combination including Applicants' executing and generating steps: "executing an application program at the node which is not secured" and "generating a message via the application program based on the input, the message representing one of a predefined set of messages for processing by a cryptographic processing component located within the node" as recited in claim 1 for reasons stated above. (Emphasis added.) MPEP § 2131 states that to anticipate a claim, the reference must teach every element of the claim. Clearly, Sudia does not teach Applicants' executing step because it does not teach executing an application program at a node that is not secured. Therefore, any "node" in Sudia in which the cryptographic processing component is located is not equivalent to Applicants' *unsecured* node wherefore Applicants' message generating step calling for processing within that unsecured node is not taught. Since at least these claim elements are not taught by Sudia, it is respectfully requested that the rejection of claim 1 under 35 USC § 102(b) be withdrawn and the claim allowed.

The other independent claims 5, 9, 13, 14 and 22 have been similarly amended, where each independent claim contains a similar limitation relating to its equivalent node (i.e., equivalent to the node which performs the method of Applicants' claim 1) that it is not secured. In addition to that language appearing in preambles of these claims, that language now appears in all of the bodies of these claims. Therefore, that language must

now be given patentable weight. Accordingly, the other independent claims are urged to be likewise allowable for reasons similar to those given above with respect to claim 1.

It is respectfully submitted that claims 2-4 dependent from claim 1, claims 6 and 8 dependent from claim 5, claims 10-12 dependent from claim 9, and claims 15-21 dependent from claim 14 are also allowable, at least for reasons based on their dependencies from allowable base claims. Furthermore, these dependent claims are independently allowable because they recite additional features not disclosed or suggested by Sudia as detailed in a previous response dated June 29, 2004, where those reasons need not be repeated here.

Therefore, in view of the foregoing, it is respectfully submitted that all independent and dependent claims are allowable over cited reference Sudia.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration and allowance are respectfully requested. Applicants respectfully request withdrawal of the outstanding rejections and the timely allowance of this application.

This amendment should be entered under Rule 116 because the scope of the amended claims is not changed and no further searching is required. The only change is from not highly secured to not secured, the change being suggested in the Office Action. Even if the Examiner is not persuaded to allow the application, entry of this amendment shall narrow down the issues to be presented on appeal.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-2347 and please credit any excess fees to such deposit account.

Respectfully submitted,

By: _____
Joel Wall
Reg. No. 25,648

Date: January 25, 2006
Verizon Corporate Services Group Inc.
600 Hidden Ridge Drive
Mail Code HQE03H14
Irving, Texas 75038
(972) 718-4800
CUSTOMER NO. 32127